Homomorphism Theorems.

Natural Homomorphism: (Qazi- 82)

Let H be a normal subgp of a group G, then the mapping $\varphi: G \longrightarrow G/H$ defined by $\varphi(g) = gH$ is called natural or Canonical homomorphism of G onto G/H.

Remark:- To every factor group G/H, there is a homomorphism $\varphi: G \longrightarrow G/H$ such that $\varphi(G) = G/H$.

Theorem: (Fundamental theorem of homomorphism) homomorphism theorem or 1st Isomorphism theorem)

Let $\varphi: G \longrightarrow G'$ be an epimorphism (onto homomorphism) from G to G'. Then.

(a) the $K = \ker\varphi$ is normal subgroup of G.

(b) the factor group G/K is isomorphic to G' i.e $\varphi(G) \cong G/K$

(c) A subgroup H' of G' is normal in G' iff its inverse image $H = \varphi^{-1}(H')$ is normal in G.

(d) There is one-one correspondence between the subgroup of G' (containing) and those sub-groups of G which contain the kernel $K = \ker\varphi$.

Proof:-

(a) To show that $K = \ker\varphi = \{k \in G : \varphi(k) = e'\}$ is a normal subgroup of G, we first we show that K is a subgroup of G.

Let $k_1, k_2 \in K$. Then

$$\varphi(k_1) = e' \quad \varphi(k_2) = e'$$

$$\text{and } \varphi(k_1 k_2^{-1}) = \varphi(k_1)(\varphi(k_2))^{-1}$$
$$= e' \cdot e'^{-1} = e' \cdot e' = e' \in G'$$

$\Rightarrow k_1 k_2^{-1} \in K$ and K is sub-group.

Next we show that K is normal in G.

For this let $k \in K$, $g \in G$. Then

$$\varphi(gkg^{-1}) = \varphi(g) \cdot \varphi(k) \cdot \varphi(g^{-1})$$
$$= \varphi(g) \cdot e' \cdot (\varphi(g))^{-1}$$
$$= e' \in G'$$

$\Rightarrow gkg^{-1} \in K$. Therefore K is normal in G.

(b) We show that $G/K \cong G'$

For this define a mapping $\psi : G/K \longrightarrow G'$ as follows.

For any $gK \in G/K$, $g \in G$ we put

$$\psi(gK) = \phi(g)$$

Then for $g_1K, g_2K \in G/K$

$$\begin{aligned}\psi((g_1K)(g_2K)) &= \psi(g_1g_2K)\\ &= \phi(g_1g_2)\\ &= \phi(g_1)\psi(g_2) \quad (\because \phi \text{ is hom.})\\ &= \psi(g_1K)\cdot\psi(g_2K)\end{aligned}$$

Hence ψ is a homomorphism and $G/K \cong G'$

(C) Suppose H' is normal in ~~in~~ G' and

$$H = \phi^{-1}(H') = \{h \in G : \phi(h) = h' \in H'\}$$

Since $K = \ker\phi$ is inverse image of e'

$\therefore$ K is contained in H.

Let $h \in H$ and $g \in G$. Then $ghg^{-1} \in H$ ~~$\because H$ is normal in G~~

iff $\phi(ghg^{-1}) \in H'$ ~~$\therefore ghg^{-1} \in H$~~

But $\phi(ghg^{-1}) = \phi(g)\cdot\phi(h)\cdot\phi(g^{-1})$

$= \phi(g)\cdot\phi(h)\cdot\phi(g)^{-1} \in H' \quad (\because H' \trianglelefteq G')$

$\Rightarrow ghg^{-1} \in H$ and $H \trianglelefteq G$

Conversely suppose that H is normal in G and $H' = \phi(H)$

Let $h' \in H'$, $g' \in G'$

and $\phi(h) = h'$ $\phi(g) = g'$

$$g'h'g'^{-1} = \phi(g)\cdot\phi(h)\cdot\phi(g)^{-1}$$

$$= \phi(ghg^{-1})$$

$\because H \trianglelefteq G$

$ghg^{-1} \in H$

$\therefore$

$\Rightarrow \phi(ghg^{-1}) \in \phi(H) = H'$

$\Rightarrow g'h'g'^{-1} \in H'$. Hence H' is normal in G'

(d):- Let Ω be the collection of all sub-groups of G containing K and Ω' be the collection of all sub-groups of G'. Define a mapping $\alpha : \Omega \longrightarrow \Omega'$ by

$$\alpha(H) = \varphi(H) = H'$$

If $H_1, H_2 \in \Omega$ and

$$\alpha(H_1) = \alpha(H_2) = H' \text{ (say)}$$

we show that $H_1 = H_2$

Let $H_1 = \varphi^{-1}(H')$

Then $H_1 \subseteq H$.

Let $h \in H$, $\varphi(h) = h' = \varphi(h_1)$

From $\alpha(H_1) = H' = \varphi(H_1)$, for $h' \in H'$, $h_1 \in H_1$

Hence

$$h_1^{-1} h \in K$$

i.e. $h \in h_1 K \subseteq H_1$.

Thus $H \subseteq H_1 \Rightarrow H = H_1$

Similarly $H = H_2$.

Hence α is injective.

Also each $H' \in \Omega'$ is the image of an $H = \varphi^{-1}(H')$. Hence α is surjective.

Thus α is one-one correspondence

Kernel of φ: Let $\varphi : G \longrightarrow G'$ be a homomorphism. The set of all those elements of G which are mapped onto the identity e' of G' is called the kernel of φ & is denoted by $\ker\varphi$. Thus

$$\ker\varphi = \{k \in G : \varphi(k) = e'\} = \{k = \varphi^{-1}(e')\}$$

Theorem:- Let $\varphi : G \longrightarrow G'$ be a homomorphism of G onto G'. Then

(a) If H is a sub-group of G, then $\varphi(H)$ is a sub-group of G'

(b) If H is normal in G, $\varphi(H)$ is normal in G'

Proof: (a) Since $\varphi(e) \in \varphi(H)$

$$\therefore \varphi(H) \neq \phi.$$

Let $x_1, x_2 \in \varphi(H)$

$\Rightarrow x_1 = \varphi(h_1)$ $x_2 = \varphi(h_2)$ for

Then $x_1x_2^{-1} = \phi(h_1)(\phi(h_2))^{-1} = \phi(h_1).\phi(h_2^{-1}) = \phi(h_1h_2^{-1}) \in \phi(H)$

$\Rightarrow \phi(H)$ is a sub-group.

(b) Let $H \trianglelefteq G$

then $ghg^{-1} \in H \quad \forall g \in G, \forall h \in H$

Now any element of G' is of form $\phi(g)$ for some $g \in G$; and any element $\phi(H)$ is of the form $\phi(h)$ for som $h \in H$

Now

$$\phi(g)(\phi(h))\phi(g)^{-1}$$
$$= \phi(ghg^{-1}) \in \phi(H) \quad \because ghg^{-1} \in H$$

Thus $\phi(H) \trianglelefteq G'$.

Theorem: (Correspondence theorem)

Let $\phi: G \longrightarrow G'$ be a homomorphism of G onto G', Then

(a) the preimage H of a any sub-group S of G' is a sub-group of G containing $\ker\phi$

(b) If $S \trianglelefteq G'$, then $H \trianglelefteq G$. Furthermore if H_1 is any other sub-group of G containing $\ker\phi$ such that $\phi(H_1) = S$, then $H_1 = H$.

Proof:

(a) $H = \{g \mid \phi(g) \in S\}$

Since $\phi(e)$ is identity of G' and S contains identity of G', therefore $e \in H$. So $H \neq \phi$.

Let $h_1, h_2 \in H$

then $\phi(h_1h_2^{-1}) = \phi(h_1).(\phi(h_2))^{-1} \in S \quad \because \phi(h_1) \in S$, $\phi(h_2)^{-1} \in S$

$\Rightarrow h_1h_2^{-1} \in H$

$\Rightarrow H$ is a sub-group of G.

Since $\ker\phi = \{x \mid \phi(x) = e' \in G'\}$ and $e' \in S$

$\therefore \ker\phi \subseteq H$.

(b) Let $S \trianglelefteq G'$. We are to show that $H \trianglelefteq G$.

Let $h \in H, g \in G$

$\phi(ghg^{-1}) = \phi(g)\,\phi(h)\,(\phi(g))^{-1}$

Since $\phi(g) \in G'$ and $\phi(h) \in S$, $S \trianglelefteq G'$

Thus all the cosets are distinct

Let $g \in G$

Then $\phi(g) \in G'$

and so $\phi(g) \in Sg_i'$ for some integer i

$\Rightarrow \phi(g) = sg_i'$, $s \in S$

Consider $x = gg_i^{-1}$

$\phi(x) = \phi(gg_i^{-1}) = \phi(g)\phi(g_i^{-1})$

$= sg_i'g_i'^{-1} = s$

$\Rightarrow gg_i^{-1}$ is the preimage of S

so that $gg_i^{-1} \in H$

$\Rightarrow g \in Hg_i$

$\Rightarrow$ Every element of G is member of one of cosets $Hg_i : i = 1, 2, \ldots n$. Hence these cosets constitute the totality of cosets of H in G. Hence index of H in G is also n

Corollary:-2: Let $N \trianglelefteq G$ and L be a subgroup of G/N. Then we can write $L = H/N$, where H is a subgroup of G containing N. If $L \trianglelefteq G/N$, then $H \trianglelefteq G$. If $H_1/N = H/N$ where H_1 & H are sub-groups of G containing N, then $H_1 = H$.

Proof:-

Let $f: G \longrightarrow G/N$ be the natural homomorphism and $H = \{g \mid f(g) \in L\}$

If $L \trianglelefteq G/N$

Then $H \trianglelefteq G$. (by correspondence theorem)

Since $f: g \rightarrow Ng$

$\therefore f(H)$ consists of all cosets Nh, $h \in H$

$\Rightarrow f(H) = L$

Because $H \supseteq N = \ker f$ (by correspondence theorem)

Therefore H/N makes sense and consists of all the cosets Nh, $h \in H$. Hence $H/N = f(H) = L$

Now if $H_1 \supseteq N$ and $H_1/N = H/N$

Then $f(H_1) = L = f(H)$

$\Rightarrow H_1 = H$ (by correspondence theorem)

$\therefore \quad \phi(g)\,\phi(h)\,(\phi(g))^{-1} \in S$

$\Rightarrow \phi(g h g^{-1}) \in S$

$\Rightarrow g h g^{-1} \in H \Rightarrow H \trianglelefteq G.$

Further let H_1 be sub-group of G containing $\ker\phi$ and $\phi(H_1) = S$. We will show that

$$H_1 = H$$

Let $h_1 \in H_1$

$\Rightarrow \phi(h_1) \in S$

$\Rightarrow h_1 \in H$

$\Rightarrow H_1 \subseteq H \longrightarrow$ (A)

If $h \in H$, then $\phi(h) = s \in S$

Choose $h_1 \in H_1$ such that

$$\phi(h_1) = s$$

Then $h h_1^{-1} \in \ker\phi \subseteq H_1$ and so $h \in H_1$

and $H \subseteq H_1 \longrightarrow$ (B)

By (A) & (B)

$$H_1 = H$$

Corollary:-1. Let $\phi: G \longrightarrow G'$ be an onto homomorphism and S be a subgroup of G' of index $n < \infty$. Let H be the preimage of S. Then H is of index n in G.

Proof:- Let $Sg_1', Sg_2', Sg_3', \ldots, Sg_n'$, where $g_i' \in G'$ be the distinct cosets of S in G'. As ϕ is onto, there are $g_1, g_2, g_3, \ldots g_n \in G$ such that

$$\phi(g_i) = g_i' \quad i = 1, 2, \ldots n$$

We claim that

$Hg_1, Hg_2, \ldots Hg_n$ are distinct cosets of H in G

Let $Hg_i = Hg_j$

Then $g_i g_j^{-1} \in H$

$\Rightarrow \phi(g_i g_j^{-1}) = \phi(g_i)(\phi(g_j))^{-1} \in S$

i.e $g_i' g_j'^{-1} \in S$

$\Rightarrow Sg_i' = Sg_j'$

$\Rightarrow i = j$

So $Hg_i = Hg_i \Rightarrow g_i = g_j$

Problem: Let $\varphi : G \to G'$ be an onto homomorphism. Let G' be a cyclic group of order 10. Prove that G has normal sub-groups of index 2, 5, and 10

Solution:- Let $G' = gp(g')$. Then the sub-groups $G_1' = \{e\}$, $G_2' = gp(g^5)$, $G_3' = gp(g^2)$ are normal subgps of G' of index 10, 5 and 2 respectively. Consequently their preimages, by correspondence theorem are normal of index 10, 5 and 2 respectively.

Problem:- Let H be a sub-group of index n in G. Let $\varphi : G \to G'$ be an onto homomorphism. Prove that $\varphi(H)$ is of index n in G' if $H \supseteq \ker\varphi$.

Solution:- We only prove that $\varphi(H) = S$ is of finite index in G', for then the result follows from corollary (4) of correspondence theorem.

If $Hg_1, Hg_2, \ldots\ldots Hg_n$ are the cosets of H in G. Then we show that $S(\varphi(g_1)), S(\varphi(g_2)) \ldots\ldots S(\varphi(g_n))$ is the totality of cosets of S in G'.

Let $g' \in G'$

Then $\varphi(g) = g'$ for some $g \in G$, as φ is onto

Let $g = hg_i$, Then $g' = \varphi(g) = \varphi(h)\,\varphi(g_i) \in S(\varphi(g_i))$

$\Rightarrow$ Every element of G' is contained some $S(\varphi(g_i))$.

Hence the result

Alternatively we can show that $S(\varphi(g_1)) \ldots$ $S(\varphi(g_n))$ are all distinct

Suppose $S(\varphi(g_i)) = S(\varphi(g_j))$

Then $\varphi(g_i)(\varphi(g_j))^{-1} = \varphi(g_i g_j^{-1}) \in S$

Hence $g_i g_j^{-1} \in H$ as H by correspondence theorem is preimage of S

$\Rightarrow$ $Hg_i = Hg_j$

$\Rightarrow$ $i = j$

Hence index of S in G' is n

Problem:- Let G be a group and let N be a normal subgroup of G. Suppose further that L and M are sub-groups of G/N. Then we can show that we can write L in the form H/N, and M in the form K/N, where H and K are sub-groups of G containing N. Show also that if $L \subseteq M$, $H \subseteq K$; and if $L \trianglelefteq M$, $H \trianglelefteq K$. Show that if $L \subseteq M$ and $[M:L] = n < \infty$, then $[K:H] = n$.

Solution: By Corollary 2 of correspondence theorem
$$L = H/N \quad \text{and} \quad M = K/N.$$
Let φ be natural homomorphism. We recall that
$$H = \{g \mid \varphi(g) \in L\} \text{ and } K = \{g \mid \varphi(g) \in M\}$$
Hence if $L \subseteq M$, $H \subseteq K$ follows immediately.

Now if $L \trianglelefteq M$

we consider the homomorphism
$$\psi : K \longrightarrow K/N \text{ defined by}$$
$$\psi(k) = \varphi(k)$$
i.e $\psi = \varphi|_K$

Clearly $\psi(K) = K/N$

and the preimage of L is H, the preimage of M is K. We can then conclude from the correspondence theorem that $H \trianglelefteq K$.

Problem:-

Let $N \trianglelefteq G$ and suppose G/N is cyclic of order 6. Let $G/N = gp(Nx)$. Find all subgroups of G/N and express them in the form Corollary 2 of Correspondence theorem.

Solution:- Let $G/N = K$, Let $K_1 = \{N\}$, $K_2 = \{N, Nx^3\}$
$$K_3 = \{N, Nx^2, Nx^4\} \text{ and } K_4 = K.$$
These are all sub-groups of K.

To find the corresponding sub-groups Corollary 2

Let $\varphi : G \longrightarrow G/N$ be natural homomorphism i.e
$$\varphi(g) = Ng.$$
Let G_i be the preimage of K_i $i = 1,2,3,4$

$G_1 = \{g \mid \varphi(g) = N\} = \{g \mid Ng = N\} = \{g \mid g \in N\} = N$

$G_2 = \{g \mid \varphi(g) = N \text{ or } g = Nx^3\} = \{g \mid Ng = N \text{ or } Ng = Nx^3\} = N \cup Nx^3$

$G_3 = \{g \mid \varphi(g) = N \text{ or } \varphi(g) = Nx^2 \text{ or } \varphi(g) = Nx^4\} = N \cup Nx^2 \cup Nx^4$

$G_4 = \{ g \mid \varphi(g) \in K \} = G$. Then $G_i/N = K_i$ for $i = 1, 2, 3, 4$.

The Subgroup isomorphism Theorem:

In homomorphism we were able to say

(i) that the image of a homomorphism $\varphi : G \to G'$ was essentially a factor group of G.

What can we say about the effect of φ on sub-groups? Let H be a sub-group of G. Let $\psi = \varphi|_H$ i.e. ψ is the mapping of H to G' defined by

$$\psi(h) = \varphi(h), \; h \in H$$

Then ψ is a homomorphism of $H \to G'$ and

so $\quad \psi(H) = \varphi(H) \cong H/(\ker \psi)$

Now if $\ker \varphi = N = \{ x \mid x \in G, \varphi(x) = e' \}$.

Then $\quad \ker \psi = \{ x \mid x \in H \text{ and } \psi(x) = \varphi(x) = e' \} = H \cap N$

So $\quad \varphi(H) = \psi(H) \cong H/(H \cap N)$. On the other hand, we know that $\varphi(H)$ is a subset of $\varphi(G)$ and

$$\varphi(G) \cong G/N.$$

Our question is; what has $H/(H \cap N)$ got to do with G/N? It must be isomorphic to some subgroup of G/N. But which. This is what the sub-group isomorphism theorem is.

Theorem (Subgroup Isomorphism Theorem, also called the Second isomorphism theorem).

Let A, B be sub-groups of a group G with A normal in G, Then.

(i) $\langle A, B \rangle = AB$ is a sub-group

(ii) $A \cap B$ is normal sub-group of B

(iii) $AB/A \cong B/A \cap B$

Proof:- (i) Let A, B be sub-groups of G and A normal in G, then we first show that

$$\langle A, B \rangle = AB$$

Now each element of $\langle A, B \rangle$ is of the form

$x = a_1^{\alpha} b_1 a_2 b_2 a_3 b_3 \ldots a_k b_k^{\beta}$ where α, β are 0 or 1, $a_i \in A, b_i \in B$, $1 \le i \le k$

Since A is normal in G

$\therefore \quad bab^{-1} \in A \qquad \forall a \in A, \forall b \in B.$

$\Rightarrow \quad bab^{-1} = a' \qquad$ for some $a' \in A$.

$\Rightarrow \quad ba = a'b$

So $\quad x = a_1^{\alpha} a_2' a_3' \cdots a_k' \, b_1 b_2 \cdots b_k^{\beta}$

$\quad x = ab \qquad a \in A \qquad b \in B$

Thus $\quad x \in AB$

$\Rightarrow \langle A, B \rangle \subseteq AB$

Conversely each $ab \in AB$ is in $\langle A, B \rangle$.

So $\quad AB \subseteq \langle A, B \rangle$

Hence $\langle A, B \rangle = AB$

(ii) To show that AB is a sub-group of G.

Let $x, y \in AB$

Then $x = ab \quad y = a'b' \qquad x, y \in AB$

$\qquad a, a' \in A, \; b, b' \in B$

$$
\begin{aligned}
xy^{-1} &= ab \cdot (a'b')^{-1} \\
&= ab \cdot (b'^{-1} a'^{-1}) \\
&= a b b'^{-1} a'^{-1} \\
&= a b_1 a'^{-1} && b_1 = b b'^{-1} \in B \\
&= a a'^{-1} b_1 && \because A \text{ is normal} \\
&= a_1 b_1 \in AB && \therefore b_1 a'^{-1} = a'^{-1} b_1 \\
& && ; \; a_1 = a a'^{-1} \in A
\end{aligned}
$$

Hence AB is sub-group of G.

OR

Since A is normal in G,

$\therefore \quad AB = BA$

$\Rightarrow AB$ is a sub-group of G (by a previous theorem)

(iii)

Since A & B are sub groups of G, $A \cap B$ is a sub-group of G. To show that $A \cap B$ is normal in B

Let $x \in A \cap B$ & $b \in B$, then

$bxb^{-1} \in A \qquad \because A \trianglelefteq G$

$bxb^{-1} \in B \qquad \because B$ is sub gp.

So that

$bxb^{-1} \in A \cap B \qquad \forall x \in A \cap B, \forall b \in B$

Hence $A \cap B$ is normal in B.

(iii) To prove $AB/A \cong B/A \cap B$

Every element of AB/A is of the form

$abA = ba'A \quad \because A \trianglelefteq G$

$= bA \quad b \in B \quad \because ab = ba'$

Also let $D = A \cap B$

Then every element of $B/A \cap B = B/D$ is of the form bD, $b \in B$

We define a mapping $\psi : AB/A \longrightarrow B/D$ as

$\psi(bA) = bD$, $b \in B$

First we show that ψ is well defined

For this suppose that

$bA = b'A$

We have to show that $bD = b'D$

Now.

$bA = b'A \Rightarrow b'^{-1}bA = A$

$\Rightarrow b'^{-1}b \in A$

But $b'^{-1}b \in B$

Hence

$b'^{-1}b \in A \cap B = D$ or $b'^{-1}b \in D$

So $b \in b'D$ But $b \in bD$

$\Rightarrow b'D \cap bD \neq \phi$

Hence $bD = b'D$

So ψ is obviously well defined

Next ψ is obviously surjective

To see that ψ is injective

Suppose that

$\psi(bA) = \psi(b'A)$ for some $b, b' \in B$

Then $bD = b'D$

$b'^{-1}bD = D$

i.e $b'^{-1}b \in D$

or $b'^{-1}b \in D = A \cap B$ So $b'^{-1}b \in A$

i.e $b \in b'A$

But $b \in bA$ also

Hence $bA = b'A$ $\because (bA) \cap (b'A) \neq \phi$

So ψ is injective.

Lastly for $bA, b'A \in AB/A$, $bb' \in B$, we have

$$\psi(bA \cdot b'A) = \psi((bb')A)$$
$$= (bb')D = bD \cdot b'D$$
$$= \psi(bA) \cdot \psi(b'A)$$

So ψ is homomorphism

As ψ is bijective & homomorphism

So $AB/A \cong B/A \cap B$

<u>OR</u>

Let $\varphi : B \longrightarrow AB/A$ be defined by

$$\varphi(b) = bA$$

Then $\varphi(bb') = bb'A = bA \cdot b'A$
$$= \varphi(b) \cdot \varphi(b')$$

$\Rightarrow \varphi$ is homomorphism.

Let $hA \in AB/A$, where $h \in AB$

Now $h \in AB$ gives

$$h = a_1 b_1 \quad a_1 \in A,\ b_1 \in B$$

Thus $hA = a_1 b_1 A = b_1 a' A$ $\quad \because A$ is normal
$$= b_1 A = \varphi(b_1)$$

$\Rightarrow \varphi$ is also onto i.e $\varphi(B) = AB/A$

G. By fundamental theorem of homomorphism

$\varphi(B) \cong B/(\ker\varphi)$ $\quad$ i.e $AB/A \cong B/(\ker\varphi)$

(Shaum, outli)

$\ker\varphi = \{x \mid x \in B;\ \varphi(x) = e'\}$ $\quad e' = eA = A$

$= \{x \mid x \in B,\ xA = A\}$ $\quad \because \varphi(x) = xA$ & $\cancel{\varphi(eA) = \varphi(A)} =$

If $xA = A$, then $x.e = x \in A$ and if $x \in A$, $xA = A$.

Therefore $\ker\varphi = \{x \mid x \in B,\ x \in A\} = B \cap A$.

Hence

$$\varphi(B) \cong \frac{B}{B \cap A}$$

$$AB/A \cong B/B \cap A.$$

G <u>OR</u>

(Qazi, 83) $\quad$ Now A is identity of AB.

So for any $b \in B$, $b \in \ker\varphi$

$\Leftrightarrow \quad \varphi(b) = A$

$\Leftrightarrow \quad bA = A$

$\Leftrightarrow \quad b \in A$

$\Leftrightarrow \quad b \in A \cap B$; since $b \in B$

i.e $b \in \ker\varphi \Leftrightarrow b \in A \cap B$

$\Rightarrow \quad \ker\varphi = A \cap B$

Hence $AB/A = B/A\cap B$

Problem:- Let Q^* be the multiplicative grop of rationals. Let $N = \{1, -1\}$. Let H be the sub-gp generated by $(1/2)$. Find HN, HN/N and thereby the assertion of the sub-gp isomorphism theorem that

$HN/N = H/H\cap N$

Solution:- The elements of H are the form $(\frac{1}{2})^r$, r various integers.

$HN = \{x \mid x = hn,\ h \in H,\ n \in N\} = \{x \mid x = h \text{ or } x = -h, h \in H\}$

$= \{x \mid x = \pm(1/2)^r \text{ for all integers } r\}$

Cosets of HN/N is of the form

$Nx = \{1, -1\}x = \{x, -x\}$ where $x \in HN$

Now if $x \in HN$, $x = \pm(1/2)^r$

Hence each coset is of the form

$\{(1/2)^r, -(1/2)^r\}$.

Since $N(1/2) \cdot N(1/2) \cdot N(1/2) \cdots N(1/2) = N(1/2)^r$ and $(1/2)^r \in N(1/2)^r$, each coset of HN/N is a power of $N(1/2)$.

Thus

$$gp(\{N(1/2)\}) = HN/N$$

Since $(\frac{1}{2})^r \notin N$ for $r \neq 0$

$\therefore$ HN/N is the infinite cyclic gp.

Now $H \cap N = \{x \mid x = (\frac{1}{2})^r \text{ for some } r \text{ and } x = \pm 1\}$

$= \pm 1$

$H/(H\cap N) \cong H$

But H is infinite cyclic.

Thus $H/(H\cap N) \cong HN/N$

Problem Let a group G contains two normal sub-groups M & N. Let H be a sub-group of G. Prove that $HM/M \cong HN/N$ if $H\cap M = H\cap N$.

Solution: By sub-group isomorphism theorem

$$HM/M \cong H/H\cap M = H/H\cap N \cong HN/N$$

$$\Rightarrow HN/N \cong HM/M$$

Remark: If G/M has every element of order a power of 2, show that $H/H\cap N$ has every element of order a power of 2

Solution

$$H/H\cap N = H/H\cap M \cong HM/M \subseteq G/M$$

Hence the result.

Problem: Let H and K be subgroups of G, $N \trianglelefteq G$ and $HN = KN$. Prove that $H/(H\cap N) \cong K/(K\cap N)$.

Solution:

Since H, N are subgroups of G and $N \trianglelefteq G$

$\therefore$ By sub-group isomorphism theorem

$$H/(H\cap N) \cong HN/N \longrightarrow ①$$

Also since K, N are subgroups of G and $N \trianglelefteq G$

$\therefore$ By Sub-group isomormphism theorem

$$K/(K\cap N) \cong KN/N \longrightarrow ②$$

Since $HN = KN$

Therefore by ① & ②

$$H/(H\cap N) \cong K/(K\cap N)$$

($\because$ Two sub-groups isomorphic to same gp are isomorphic)

Problem:- Let $G \supseteq G_1 \supseteq G_2 \supseteq \{1\}$. Let $G_1 \trianglelefteq G$, $G_2 \trianglelefteq G_1$ and suppose G/G_1, G_1/G_2 and G_2 are abelian. Prove that if H is any sub-group, then it has subgroup $H_1 \& H_2$ such that $H_1 \trianglelefteq H$, $H_2 \trianglelefteq H_1$ and H/H_1, H_1/H_2 and H_2 are abelian.

Solution:- Let $H_1 = H \cap G_1$

Then by sub-group isomorphism theorem

$H_1 \trianglelefteq H$ and $H/H_1 \cong HG_1/G_1$

But $HG_1/G_1 \subseteq G/G_1$ and G/G_1 is abelian.

Hence H/H_1 is abelian.

Now consider H_1 as a subgroup of G_1

As $G_2 \trianglelefteq G_1$

$\therefore$ By sub-group isomorphism theorem

$H_1 \cap G_2 \trianglelefteq H_1$ and $H_1/(H_1 \cap G_2) \cong H_1G_2/G_2 \subseteq G_1/G_2$

Since G_1/G_2 is abelian

So $H_1/(H_1 \cap G_2)$ is abelian.

Consequently we put $H_1 \cap G_2 = H_2$

Finally as $H_2 \subseteq G_2$ and G_2 is abelian.

Therefore H_2 is abelian.

Problem: Let $G \supseteq G_1 \supseteq \{1\}$ and $G_1 \trianglelefteq G$. Suppose G/G_1 and G_1 are abelian and H is any sub-group of G prove that there exists a sub-group H_1 of H such that $H_1 \trianglelefteq H$ and H/H_1 and H_1 are abelian.

Solution:

Let $H_1 = H \cap G_1$

Then by the Sub-group isomorphism theorem.

$H_1 \trianglelefteq H$ and $H/H_1 \cong HG_1/G_1$

But $\frac{HG_1}{G_1} \subseteq G/G_1$ and G/G_1 is abelian.

Therefore H/H_1 is abelian

As $H_1 \subseteq G_1$ and G_1 is abelian

Therefore H_1 is abelian.

Theorem (third isomorphism theorem).
(Factor of Factor theorem)

Let H & K be normal sub-groups of G and $H \subseteq K$, then K/H is normal sub-group of G/H and

$$(G/H)/(K/H) \cong G/K$$

Proof:

Since K is normal sub-group of G

$\therefore \; g^{-1}kg \in K \quad \forall g \in G, \forall k \in K$

$\Rightarrow (Hg^{-1})(Hk)(Hg) = H(g^{-1}kg) \in HK$

$\Rightarrow (Hg^{-1})(Hk)(Hg) \in K/H \quad \forall Hg \in G/H, Hk \in K/H$

$\Rightarrow$ K/H is a normal sub-group of G/H

~~Thus G/K, G/H, K/H are meaningfu~~

Also the sub-group H, being a normal sub-gp. of G, is normal in any sub-group of G containing H. In particular H is normal in K.

Thus G/H, G/K and K/H are all meaningful.

Define a mapping

$\phi : G/H \longrightarrow G/K$ by

$\phi(gH) = gK$

Then ϕ is surjective

Also

$\phi(gH \cdot g'H) = \phi(gg'H)$

$= gg'K = gK \cdot g'K$

$= \phi(gH) \cdot \phi(g'k)$

$\Rightarrow \phi$ is homomorphism.

Thus by first homomorphism theorem

$(G/H)/K' \cong G/K$

where $K' = \ker \phi$.

We show that $K' = K/H$

Obviously $K' \supseteq K/H$

Let $gH \in K'$

Let $kH \in K/H$

$\because K \subseteq G, H \subseteq G$

$\therefore \phi(kH) = kK = K$

$\Rightarrow kH \in K'$

$\therefore K' \supseteq K/H$

$\Rightarrow \quad \varphi(gH) = gK$
$= K \quad \because gH \in K'$

$\Rightarrow g \in K$

Hence $gH \in K/H$.

Thus $K' = K/H$.

Consequently

$$(G/H)/(K/H) \cong G/K$$

(Shanti 109) **Theorem:** Let H be normal sub-group of G. K is normal sub-group of G containing H iff K/H is a normal sub-group of G/H.

Solution:- Let K be sub-group of G containing H i.e.

$$H \subseteq K \subseteq G$$

Since H is normal in G.

$\therefore \quad gH = Hg \quad \forall g \in G$.

and in particular

$$gH = Hg \quad \forall g \in K.$$

$\Rightarrow$ H is a normal sub-group of K and the symbol K/H is meaningful.

Let $Hk_1, Hk_2 \in K/H$.

Then $Hk_1, Hk_2 \in G/H$.

we have

$k_1, k_2 \in K \Rightarrow k_1k_2^{-1} \in K$ ($\because K$ is sub-group)

$\Rightarrow H(k_1k_2^{-1}) \in K/H$

$\Rightarrow (Hk_1)(Hk_2^{-1}) \in K/H$.

$\Rightarrow (Hk_1)(Hk_2)^{-1} \in K/H$

$\Rightarrow K/H$ is a sub-group of G/H

~~Conversely~~ Consider any sub-gp of G/H so that the members of this sub-group are some or all of the cosets of H. Let K denote the set theoretic union of these cosets. We show that K is a sub-group of G containing H.

Let $x_1, x_2 \in K$ so that Hx_1, Hx_2 are members of the sub-group of G/H in question

It follows that

$$(Hx_1)(Hx_2)^{-1} = (Hx_1x_2^{-1})$$

is as well a coset member of the sub-group G/H.

$\Rightarrow x_1x_2^{-1} \in K$

Thus K is sub-group.

Surely it contains H

Thus K/H is sub-group of G/H

Now K is a normal sub-group of G iff

$$x^{-1}kx \in K \quad \forall x \in G, \forall k \in G$$

$$\Rightarrow (Hx^{-1})(Hk)(Hx) = H(x^{-1}kx) \in Hk$$

$$\forall Hx \in G/H, Hk \in K/H$$

$\Leftrightarrow$ K/H is a normal sub-group of G/H

<u>Remark</u> A group G is abelian if and only if G coincides with its centre $\xi(G)$.

<u>**Theorem**</u>:- A group G is abelian if and only if the factor group $G/\xi(G)$ is cyclic.

<u>Proof</u>:-

Let G is abelian

Then $G = \xi(G)$.

So $G/\xi(G)$ is the trivial group and hence cyclic (The trivial or the identity group assumed to be generated by the empty set)

Conversely suppose that $G/\xi(G)$ is a cyclic group and $a\xi(G), a \in G$ is its generator.

Let $x, y \in G$

Then $x\xi(G), y\xi(G)$ belong to $G/\xi(G)$

So there exist integers m, n such that

$x\xi(G) = a^m\xi(G)$, $y\xi(G) = a^n\xi(G)$

Thus $x = a^m z$, $y = a^n z'$ for some $z, z' \in \xi(G)$

$$xy = a^m z a^n z' = a^m a^n z z'$$

$$= a^n a^m z' z \quad (\because \xi(G) \text{ is abelian})$$

$= a^n z . a^m z = yx.$

Consequently G is abelian

Theorem:- A group of order p^2, where p is prime number, is abelian. (It is proved in p-groups).

Problem:- If H is a normal sub-group of G, then the mapping $f: G \longrightarrow G/H$ such that $f(a) = aH \quad \forall a \in G$ is a homomorphism. Also determine its kernel.

Solution: Let $a, b \in G$

Now $f(a.b) = (ab)H$

$= (aH).(bH)$

$= f(a).f(b)$

$\Rightarrow$ f is a homomorphism.

We claim that $\ker f = K = H$

Let $k \in K = \ker f$

Then $f(k) = eH = H$ where H is identity of G/H

Let $x \in K \subseteq G$

Then $f(x) = xH$

But $f(x) = H$.

$\Rightarrow xH = H$

$\Rightarrow x \in H$

Since x is an arbitrary element of K

$\therefore K \subseteq H \longrightarrow ①$

Again let $y \in H$

Then $yH = H$

$\Rightarrow f(y) = H$

$\Rightarrow y \in \ker f = K$

$\Rightarrow H \subseteq K \longrightarrow ②$

By ① & ②

$K = H.$

~~Endomorphisms~~ & ~~Automorphisms~~

(2021'84) **Problem:-** For $a, b \in R$, $a \neq 0$, define $f: R \to R$ by $f_{ab}(x) = ax+b$. Let $G = \{f_{ab} \mid a, b \in R, a \neq 0\}$ and $N = \{f_{1b} \in G\}$. Prove that N is a normal sub-group of G and $G/N \cong$ the group of non-zero real numbers under multiplication.

Solution:- $f_{10}(x) = x$ shows that the identity mapping $I_R \in G$. So G is non empty.

Let $a, b, c, d \in R$ with $a \neq 0$, and $c \neq 0$.

Then $f_{ab}[f_{cd}(x)] = f_{ab}(cx+d) = a(cx+d)+b$

$= acx + ad+b$

Thus $f_{ab} f_{cd} = f_{ac,\, ad+b} \longrightarrow (1)$

Under this operation G is group with $(f_{ab})^{-1} = f_{a^{-1}, -a^{-1}b}$ and f_{10} as identity.

Clearly $f_{10} \in N$, so N is non empty.

Let $f_{1b}, f_{1d} \in N$

Then $f_{1b}(f_{1d})^{-1} = f_{1b} f_{1,-d}$

$= f_{1,-d+b} \in N$

So N is a sub-group of G.

Let:
$f_{ac,\, ad+b} = f_{10}$
$\Rightarrow ac = 1 \Rightarrow c = a^{-1}$
$ad+b = 0$
$\Rightarrow d = -a^{-1}b$
Hence
$(f_{ab})^{-1} = f_{a^{-1}, -a^{-1}b}$

Again if $f_{ab} \in G$, $f_{1c} \in N$

$$f_{ab} f_{1c} (f_{ab})^{-1} = f_{a,\, ac+b} f_{a^{-1}, -a^{-1}b}$$

$$= f_{1,\, ac} \in N$$

Hence N is normal sub-group of G.

Finally let K be the group of non-zero real numbers under multiplication.

Define $\theta: G \to K$ by

$\theta(f_{ab}) = a \quad \forall f_{ab} \in G$

Clearly θ is onto

$\theta(f_{ab} f_{cd}) = \theta(f_{ac,\, ad+b}) = ac = \theta(f_{ab})\theta(f_{cd})$

$\Rightarrow \theta$ is a homomorphism.

$f_{ab} \in \ker\theta \Leftrightarrow \theta(f_{ab}) = \text{identity of } K$

$\Leftrightarrow a = 1$

$\Leftrightarrow fab = f1b$

$\Leftrightarrow fab \in N$

Hence $\ker\theta = N$

By fundamental theorem of homomorphism

$G/N \cong K$

Commutator or Derived Sub-groups

Commutator Let G be a group and $a, b \in G$ then the element $aba^{-1}b^{-1}$ is called the commutator of elements a & b and is denoted by $[a\, b]$.

Derived or First Derived Group

The group generated by all the commutators $[a, b]$, $a, b \in G$ is called the commutator sub-gp of G or the first derived group of G and is denoted by G' or G^c.

Theorem prove that the inverse of a commutator is a commutator.

Proof: $[a\ b] = aba^{-1}b^{-1} = z$ say.

So $z^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b\ a]$

Theorem The following commutator identities hold in a group:

i) $[ab]^{-1} = [b\ a]$

ii) $[ab, c] = [b \cdot c]^a [a, c]$

iii) $[a\ bc] = [a\ b][a, c]^b$

iv) $[a, b^{-1}] = [b\ a]^{b^{-1}}$ and

$[a^{-1}\ b] = [b\ a]^{a^{-1}}$ $\forall\ a, b, c \in G$

Here x^a denotes the conjugate axa^{-1} of x.

Proof:-

(i) Since $[a\ b] = aba^{-1}b^{-1}$

$\Rightarrow [a\ b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b\ a]$

(ii) $[ab, c] = abc(ab)^{-1}c^{-1}$

$= abcb^{-1}a^{-1}c^{-1}$

$= a(bcb^{-1})(ca)^{-1}$

$= a(bcb^{-1})c^{-1}c(ca)^{-1}$

$= a(bcb^{-1}c^{-1})a^{-1}ac(ca)^{-1}$

$= a(bcb^{-1}c^{-1})a^{-1}\ aca^{-1}c^{-1}$

$= [b\ c]^a [a\ c]$

Remark: ①: The commutator of two elements a, b is identity iff a & b commute.
②: Every element conjugate to a commutator is a commutator.

---

iii) $[a\ bc] = a(bc)a^{-1}(bc)^{-1}$
$= abca^{-1}c^{-1}b^{-1}$
$= aba^{-1}aca^{-1}c^{-1}b^{-1}$
$= aba^{-1}b^{-1}b(aca^{-1}c^{-1})b^{-1}$
$= [a\ b][a\ c]^{b}$

(iv) $[a\ b^{-1}] = ab^{-1}a^{-1}b$
$= b^{-1}bab^{-1}a^{-1}b$
$= [b\ a]^{b^{-1}}$

and similarly $[a^{-1}\ b] = [b\ a]^{a^{-1}}$

Theorem: A group G is abelian iff $G' = \{e\}$
i.e iff $[a\ b] = e \quad \forall\ a, b \in G$

Proof: Suppose G is abelian and $a, b \in G$.
Then $ab = ba$
$\therefore [a\ b] = aba^{-1}b^{-1} = baa^{-1}b^{-1} = e$.
$\Rightarrow G'$ is sub-gp of G generated by e and $G' = e$
If $G' = e$, then in particular any Commutator $[a\ b] = aba^{-1}b^{-1} = e$
$\Rightarrow aba^{-1}b^{-1} = e$
$\Rightarrow ab = ba$
$\Rightarrow G$ is abelian.

Theorem Let G be a group. Then
(a) the derived group G' is a normal sub-gp of G
(b) the factor group G/G' is abelian
(c) If K is normal sub gp of G s.that G/K is abelian then $K \supseteq G'$

Proof To show that G' is normal in G, we have to show that for each Commutator q in G' and $g \in G$, $gqg^{-1} \in G'$

$q = aba^{-1}b^{-1} \qquad a, b \in G$

So $gqg^{-1} = gaba^{-1}b^{-1}g^{-1}$
$= \underline{gag^{-1}}\ \underline{gbg^{-1}}\ \underline{ga^{-1}g^{-1}}\ \underline{gb^{-1}g^{-1}}$
$= [a^{g}, b^{g}]$ is an element of G'

Hence G' is normal in G.

(b) Let $aG', bG' \in G/G'$.

Then

$$[aG' \; bG'] = aG' bG' (aG')^{-1} (bG')^{-1}$$
$$= ab a^{-1} b^{-1} G'$$
$$= G' \quad \because ab a^{-1} b^{-1} \in G'$$

Thus $[aG' \; bG'] = G'$, identity of G/G'

$\Rightarrow G/G'$ is abelian

OR

$$ab a^{-1} b^{-1} G' = G'$$
$$\Rightarrow (ab) G' = ba G'$$
$$\Rightarrow aG' . bG' = bG' . aG' \text{ i.e } G/G' \text{ is abelian.}$$

(c) Suppose that for any normal sub-group K of G G/K is abelian.

To show that $G' \subseteq K$. We have only to prove that every commutator $[a, b] \in K$.

Since G/K is abelian

$$\therefore ak . bK = bK . ak$$
$$(ak . bK) a^{-1}K b^{-1}K = K$$
$$(ab a^{-1} b^{-1}) K = K$$
$$\Rightarrow [a \; b] \in K$$

Hence $G' \subseteq K$

Shaum (116)

Theorem: If G is abelian, then $G/G' \cong G$

Proof:-

G' is the sub-group generated by the Commutators $ab a^{-1} b^{-1}$, $a, b \in G$

As G is abelian

Therefore $ab a^{-1} b^{-1} = ab b^{-1} a^{-1} = e$

$\Rightarrow G'$ is sub-gp generated by e

Since any product e and its inverse is again e, $G' = \{e\}$

Let ϕ be the natural homomorphism of G to G/G'

To show ϕ is isomorphism we need only show that it is one-one.

Let $\phi(a_1) = \phi(a_2)$

$\Rightarrow e a_1 = e a_2$

$\Rightarrow a_1 = a_2$

$\Rightarrow \phi$ is $(1-1)$

Thus ϕ is an isomorphism.

Shanti (88) **Theorem** A quotient group G/H is abelian iff H contains the commutator sub-group of G.

Proof: Suppose that G/H is abelian and $aH, bH \in G/H$

Then
$$aH \cdot bH = bH \cdot aH$$
$$(ab)H = (ba)H$$
$$H = (ab)^{-1}(ba)H$$
$$= (b^{-1}a^{-1}ba)H$$

$\Rightarrow b^{-1}a^{-1}ba \in H \quad \forall a, b \in G$

$\Rightarrow H$ contains every commutator and so contains G'

Conversely let G' is contained in H i.e

$ab\bar{a}^{1}b^{-1} \in H \quad \forall a, b, G$

$\Rightarrow ab\bar{a}^{1}b^{-1}H = H$

or $Hab\bar{a}^{1}b^{-1} = H$

$Hab = Hba$

$Ha \cdot Hb = Hb \cdot Ha$

$\Rightarrow G/H$ is abelian.

Shaum (118) **Theorem** If H is a subgroup of G containing G', then $H \trianglelefteq G$.

Proof Let $h \in H$ and consider $\bar{g}^{1}hg$

Now $\bar{g}^{1}hgh^{-1}$ is a commutator and belonges to G' and thus to H

Therefore $\bar{g}^{1}hgh^{-1} \cdot h = \bar{g}^{1}hg \in H$ and $H \trianglelefteq G$

OR

Let $\phi: G \to G/G'$ be natural homomorphism, then ϕ is onto. G/G' is abelian. Any sub-group of G/G'

is therefore normal and thus $\phi(H) = S$ is normal in G/G'. By the correspondence, H is the preimage of S. Hence using the correspondence theorem once more, H is normal in G.

P- Group

Let p be a prime. A gp G is a a p-group if every element in G has order a a power of the prime p.

OR

Let p be a prime. A finite p-group is is a group of order p^α, $\alpha \geq 1$

P-Sub-group A sub-gp of a gp G is a p-sub-group of G if the sub-group is itself a p-group

OR

Let G be a finite group of order n and p a prime divisor of of n. A sub-gp H of G is called a p-sub-gp if H is p-sub-gp.

Sylow p-Sub-group of G

Let G be a group of order n and p a prime divisor of n. A sub-group H of G is said to be a Sylow p-sub-gp of G if H has order p^α where p^α divides n but $p^{\alpha+1}$ does not divide n.

OR

A sub-gp H of a finite group G is a Sylow

p-group iff the order of H is a power of p and the index of H is prime to p.

Double Coset

Let H & K be sub-groups of a group G and (a) an arbitrary element of G. Then set $HaK = \{hak, h \in H, k \in K\}$ is called a double coset in G modulo (H, K) determined by (a)

Theorem Let H, K be finite sub-groups of a group G. The double coset HaK contain mn/q elements, where m, n and q are the orders of the sub-groups H, K and $Q = H \cap aKa^{-1}$

Theorem (Sylow, 2nd Theorem)
Any two Sylow p-sub-groups of a group are conjugate.

Proof# Let G be a group of order n & H, K be any two Sylow p-sub-groups each of order p^α in G. Then

$n = p^\alpha m$ & $(p, m) = 1$

$\because$ G double cosets for a partition of G

③

$$G = \bigcup_{i=1}^{s} Ha_iK \qquad a_i \in G$$

$\Rightarrow |G| = |Ha_1K| + |Ha_2K| + \cdots + |Ha_sK|$.

$\because |Ha_iK| = \dfrac{p^\alpha . p^\alpha}{q_i}$

where q_i is the order of $H \cap a_iKa_i^{-1}$

$$\Rightarrow |G| = \frac{p^\alpha . p^\alpha}{q_1} + \frac{p^\alpha p^\alpha}{q_2} + \cdots + \frac{p^\alpha p^\alpha}{q_s}$$

$$n = \sum_{i=1}^{s} \frac{p^\alpha p^\alpha}{q_i} \longrightarrow (1)$$

Dividing by p^α

$$m = \sum_{i=1}^{s} p^\alpha / q_i \longrightarrow (2)$$

Now $q_i = |H \cap a_iKa_i^{-1}|$

$\Rightarrow q_i$ is order the intersection of two p-subgps

$\Rightarrow$ each term q_i is some power of p

$\Rightarrow$ R.H.S of (2) is either multiple of p or 1.

$\because$ left hand side is not divisible by p

$p^\alpha / q_i = 1$ for at least one $i = 1, 2, \ldots s$.

Let $\dfrac{p^\alpha}{q_1} = 1 \Rightarrow p^\alpha = q_1$

$\Rightarrow p^{\alpha} = q_1 = |H \cap a_1 K a_1^{-1}|$

But $H \cap a_1 K a_1^{-1}$ is a sub-gp of H of the same order as that of H so

$$H = H \cap a_1 K a_1^{-1}$$

$$\Rightarrow H \subseteq a_1 K a_1^{-1}$$

As $|H| = |K| = |a_1 K a_1^{-1}|$

$$\Rightarrow H = a_1 K a_1^{-1}$$

Hence H and K are conjugate.

<u>Corollary</u> A finite gp G has a unique Sylow p-sub-group H iff H is normal in G.

<u>Proof</u> # Let H be unique Sylow p-sub-gp and $a \in G$. Then aHa^{-1} is also a Sylow p-sub-gp by above Theorem

But H is unique Sylow p-sub-gp of G

$$\Rightarrow aHa^{-1} = H$$

$$\Rightarrow aH = Ha \quad \forall a \in G$$

$\Rightarrow$ H is normal in G.

Conversely if H is normal in G, Then

$$aHa^{-1} = H \quad \forall a \in G$$

$\because$ all Sylow p-sub-gps are of the form aHa^{-1}, $a \in G$ and all these coincide

with H. Thus H is unique Sylow-p-sub-group

Theorem # The number k of Sylow p-sub-groups of a finite group is congruent to 1 mod p and is a factor of the order of the gp.

Proof # Let H be a Sylow p-sub-group of G. Let n be the order of G. Since any two sub-gps are conjugate, the no Sylo-p-sub-gp of G is equal to the no of sub-groups in a conjugacy class of H and no of conjugacy class is equal to the index of the normaliser ($N_G(H) = N$) of H in G.

Let $|H| = p^\alpha$ $|N| = n_1$

$(G : N) = k$ we show that

$K \equiv 1 \mod p$

double coset decomposition modulo (N, H) of G.

$$G = \bigcup_{i=1}^{s} N a_i H, \quad a_i \in G$$

$$\text{Then } n = \sum_{i=1}^{s} \frac{n_1 \cdot p^\alpha}{q_i} \longrightarrow (1)$$

where $q_i = |N \cap a_i H a_i^{-1}|$

$\Rightarrow$ q_i is a power of p because it is the order of a sub-group of a p-group $a_i H a_i^{-1}$. Hence

Dividing (1) by n_1

(6)

$$\frac{n}{n_1} = \sum_{i=1}^{r} p^\alpha/q_i$$

$$k = \sum_{i=1}^{r} p^\alpha/q_i \longrightarrow (2)$$

When $(G:N) = k$.

each term on R.H.S of (2) is multiple of p or unity. However one term among the double cosets Na_iH, ~~NaH~~ is such that $NeH = NH$ let $a_1 = e$

$$Na_1H = NH = H \quad \text{as } H \subseteq N$$

and $N \cap H = H$

so $q_1 = p^\alpha = |H|$ $[\because q_1 = |N \cap a_1 H a_1^{-1}| = |N \cap H| = |H| = p^\alpha]$

and corresponding term in (2) is

$$p^\alpha/q_1 = 1$$

and

$$k = 1 + \sum_{i=2}^{r} p^\alpha/q_i \longrightarrow (3)$$

and no other term in (3) is unity

because if for some $j > 1$, $p^\alpha/q_j = 1$ in (3)

, then $q_j = p^\alpha$

and.

$N \cap a_j H a_j^{-1}$ being sub-gp of $a_j H a_j^{-1}$

and $|N \cap a_j H a_j^{-1}| = q_j = p^\alpha$

$\Rightarrow a_j H a_j^{-1} = N \cap a_j H a_j^{-1}$

So that

$$a_j H a_j^{-1} \subseteq N$$

∵ a Sylow p-sub-gp H of G is a Sylow p-sub-gp of any Sub gp Containing H

∴ H is a Sylow p-sub-gp of N.

But H is normal in its normaliser N

So H is unique Sylow p-sub-gp of N

So

$$H = a_j H a_j^{-1}$$

Thus $a_j \in N$

$$\Rightarrow \quad N a_j H = NH = N a_1 H \qquad \because a_j \in N$$

$\Rightarrow j = 1$, a contradiction.

Hence no other term in R.H.S of (3) except 1st is unity.

So $\sum_{i=2}^{k} p^d/q_i$ is a multiple of p

because each term is multiple of p

The

$$k = 1 + lp \qquad \text{for Some integer } l.$$

$$\Rightarrow K \equiv 1 \mod p$$

∴ k is the index of a Sub-group of G, k is a factor of the order of G. Proved!